امنیت اطلاعات

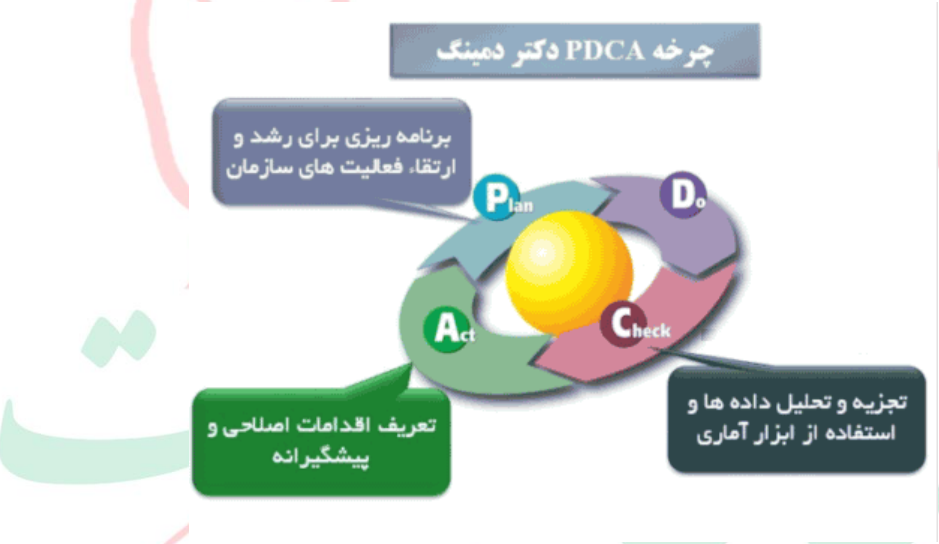
اطلاعات، با ارزش ترین و مهم ترین دارایی یک بنگاه اقتصادی و شرکت است و به واسطه اطلاعات است که شما از یک رقیب و بازار هدف صادراتی، اطلاع کسب می کنید و با آن آشنا می شوید. تا وقتی که اطلاعاتی رد و بدل نشود نمی توانید شناخت پیدا کنید. در حقیقت، اطلاعات در دنیای امروزی آنقدر مهم شده است که اگر وجود نداشته باشد نمی توانید وارد بازار شوید و کسی را به عنوان مشتری انتخاب کنید. مدیریت امنیت اطلاعات Information Security Management System (ISMS) بحث بسیار مهی است و اطلاعات در آن بسیار مهم تر است. از طرفی می گوییم Information is Knowledge به وسیله اطلاعات می توانیم دانش پیدا کنیم و از طرف دیگر می گوییم Knowledge is Power یعنی توانا بود هر که دانا بود و ترکیب این دو به این معنا است که Information is Power یعنی شما در مورد هر چیز اطلاعات داشته باشید می توانید به آن قدرت و توانایی برسید که آن موضوع را بدست بیاورید. اما امنیت اطلاعات است که باعث تضمین دوام کسب و کار شما و امنیت سرمایه گذاری می شود. زمانی که نتوانید امنیت اطلاعات خودتان را تضمین کنید یا آن را خوب مدیریت کنید، کسب و کار شما یا از بین می رود یا خدشه دار می شود. جالب است که بدانید یکی از ۱۵ مکان ممنوع دنیا که اجازه ورود به آن را ندارید، جایی که است که فرمول کوکاکولا نزدیک به ۱۰۰ سال است که در آن نگهداری می شود. کوکاکولا برای تداوم کسب و کار خود و امنیت سرمایه گذاری خود این کار را کرده چراکه مزیت رقابتی و قدرتش، در آن فرمول است اما اگر این فرمول به درستی نگهداری نمی شد شاید تا امروز کوکاکولایی وجود نداشت.

آینده تجارت کسب و کار، حالت سنتی و قدیمی خود را از دست داده و دنیای دیجیتال و فضای مجازی باعث شده که حتی اسناد صادراتی خود را هم ضمیمه یک ایمیل کنید و انتقال دهید و حتی ملاقات ها هم به صورت ویدئوکنفرانس از راه دور است و حتی پول هم الکترونیکی شده که همه اینها به سمت تجارت الکترونیک یا E-Commerce حرکت می کند. اطلاعات با یک سرعت بسیار بالایی مدام در حال ارسال و جابجا شدن است پس اهمیت اطلاعات در دنیای کسب و کار امروزی، بسیار زیاد است و برای تضمین امنیت آن باید به دنبال استانداردها رفت مانند استاندارد ISO ۲۷۰۰۱ یا مدیریت امنیت اطلاعات. البته این تنها یک روش است و هر کس می تواند از روش دیگری برای خود استفاده نمود.

اما بهتر است که چرخ را از ابتدا اختراع ننمود و از همین روش های موجود استفاده کنیم. هدف از این استاندارد که توسط موسسه ISO و IEC (که از ۱۶۰ موسسه ملی استاندارد از اقصی نقاط دنیا تشکیل شده اند) تبیین شده است، تعیین اولویت، جهت استقرار، پیاده سازی، نگهداری و بهبود مستمر سیستم مدیریت امنیت اطلاعات است و پیاده سازی آن با توجه به اندازه و ساختار بنگاه شما متفاوت خواهد بود و از محرمانگی، یکپارچگی و دسترس پذیری اطلاعات محافظت می کند. این استاندارد می گوید که باید چه اتفاقاتی بیفتد اما راه و روش آن را خودتان باید فراهم کنید. داشتن این استاندارد به مشتریان شما اطمینان خاطر می دهد که مجموعه شما نسبت به اطلاعات مشتریان، حساس است و به راحتی در اختیار همه قرار نمی دهد. علاوه بر این باعث افزایش سطح امنیت اطلاعات در سازمان می شود و فرهنگ

سازمانی شما را متناسب با این موضوعات می کند و البته باعث کاهش خطرات ناشی از سرقت اطلاعات و همچین باعث ایجاد مزیت رقابتی در صادرات در مقیاس جهانی خواهد شد..

به طور کلی، نظام مدیریتی یک سازمان در برخورد با مسائل مختلف یا یک رویکرد اقتضایی دارد یا یک رویکرد سیستماتیک و فرایندگرا. رویکرد اقتضایی به فراخور حال و اقتضای زمان، تصمیماتی می گیرد اما زمانی که مدیر بالادستی شرکت نباشد، این تصمیم گیری ها متوقف می شود چراکه سیستم، سیستماتیک و فرایندگرا نیست اما در یک سیستم فرایندگرا، شما یک سری الزامات، نیازها و انتظارات دارید که با استفاده از چرخه PDCA که از plan, Do, Check و Act تشکیل شده، قبل از راه اندازی سیستم و راه انداختن شرکت باید برنامه ریزی کنید و نقاط قوت و ضعف، اهداف، دارایی ها و توامندی های خود را بشناسید و با انجام یک سری عملیات، می توانید به حد مطلوب سیستم خود برسید. به طور کلی، بازخورد و ارزیابی عملکرد، یک نکته بسیار مهم در سیستم فرایندگرا است که در سیستم اقتضایی وجود ندارد. شما باید به صورت مداوم از کارمندان و مشتریان خود بازخورد بگیرید تا بر اساس آن ها یک سری اقدامات بهبودی انجام دهد.



سیستم ISO ۲۷۰۰۱ از ۱۴ دامنه و ۱۱۴ کنترل تشکیل شده که یک دید همه جانبه نسبت به اطلاعات دارد و البته می گوید که الزامات بالادستی سازمان شما به این ارجاعات، ارجح است بدین معنا که اگر یکی از این دامنه ها در شرکت شما کاربرد نداشته باشد می توانید آن را حذف کنید. به طور مثال می گوید که در ابتدای استخدام یک نیروی انسانی باید با هر فرد، توافقنامه منع افشای اطلاعات امضا کنید چراکه اطلاعات، جایی است که می تواند نقطه قوت یا ضعف شما باشد یا آن که کنترل دسترسی برای همه سطوح افراد، یکسان نیست. جالب است بدانید که شرکت هوآوی پورت USB همه کارمندان خود را بسته و برای تبادل اطلاعات از طریق ایمیل سازمانی اقدام می کنند و یا برای ارسال اسناد صادراتی، آیا به نظر شما بدون هیچ رمزنگاری ای، ضمیمه ایمیل می شود؟ قطعا خیر چرا که به راحتی می توان به آن اسناد دسترسی پیدا کرد در صورتی که با نرم افزار RAR و ایجاد یک رمز می توان امنیت این مطلب را بسیار افزایش داد.

به طور کلی روش های حمله و سرقت اطلاعات از چند قسمت تشکیل شده است:

روش اول، هکینگ (Hacking) است. هکرها به دو دسته هکرهای خوب و بد تقسیم می شوند. هکرهای خوب، در استخدام بسیاری از شرکت ها در می آیند تا میزان امنیت شرکت ها را از روش های خاص هکری، مورد آزمون قرار دهند اما در طرف مقابل، هکرهای بد هستند که به سیستم های شما رخنه می کنند و اطلاعات شما را به سرقت می برند.

روش دوم، فیشینگ (Phishing) یا Password Harvesting Phishing یعنی از طریق طعمه گذاری، اطلاعات و پسورد شما را بدست می آورند و برای این کار از روش های مختلفی استفاده می کنند مانند استفاده از ارسال ایمیل به این صورت که ظاهر ایمیل را طوری تغییر می دهند که شما متوجه تغییرات آن نمی شوید یا با استفاده از وب سایت های فیشینگ بدین صورت که وب سایتی شبیه یکی از وب سایت های پرداخت یا مسائل دیگر طراحی می کنند اما این سایت، اعتباری ندارد در نتیجه همه اطلاعات پرداخت و دیگر اطلاعات شما به سرقت می رود. امروز، دنیا، دنیای ارتباطات مجازی است و نرم افزارهای ارتباط مجازی مانند تلگرام، در عین حال که خیلی مفید هستند می توانند خیلی هم خطرناک باشند و با استفاده از امکان ارسال یک ویروس می توانند بسیاری از اطلاعات را هک کنند.

روش سوم، Sniffing است. یک سری هکرهایی هستند که مدام شما را Trace می کنند منتها بدون سر و صدا که شبیه یک جاسوسی بی سر و صدا می ماند. اینها منتظر هستند دیتایی از مجموعه شما خارج شود تا بتوانند آن اطلاعات را بدست آورند. به عبارت دیگر شما را مهندسی اجتماعی می کنند و بعدا از مجموعه اطلاعاتی که از مجموعه شما درز کرده علیه شما استفاده می کنند.

روش های بعدی، استفاده از تروجان، Worm، بدافزار و جاسوس افزارها، ارسال ایمیل های تشویقی و ترغیب به کلیک بر روی لینک های مختلف است. جالب است که بدانید در دنیا بیش از ۳۰٪ مردم به این ایمیل ها پاسخ می دهند و روی آن ها کلیک می کنند. مثلا ایمیلی می آید و می گوید که شما برنده فلان مورد شدید و برای گرفتن جایزه خود روی این لینک کلیک کنید یا اگر می خواهید فلان پکیج را بدست بیاورید اینجا کلیک کنید که این کار درستی نیست و نباید به هر ایمیل و لینکی اطمینان کرد. به عنوان مثال ممکن است یک ایمیل، یک جی میل باشد اما چرا برای کسی که قرار است پرداختی انجام دهم با جی میل به من ایمیل می زند؟ البته احتمال این موضوع صفر نیست اما قدری عجیب است. با دقت بیشتر متوجه می شوم که من را در Bcc ایمیل قرار داده است یعنی رونوشت مخفی. اگر من مخاطب این ایمیل بودم، دلیلی وجود نداشت که در Bcc قرار بگیرم. با دقت بیشتر متوجه می شوم که فایلی ضمیمه کرده است با پسوند xls. که شبیه اکسل است ولی پسوند اکسل xlsx است. می بینید که یک تغییر کوچک است و شما باید خیلی ریز و موشکافانه به آن دقت کنید و در نهایت می بینم که از یک وب سایتی است که هیچ سنخیتی با آن جی میل ندارد. در کنار هم قرار دادن این چهار مورد، متوجه می شوم که این ایمیل، یک ایمیل فیشینگ است و حتی گوگل هم به من پیغام داده است که مراقب باشید شاید این ایمیل، قابل اطمینان نباشد. در مثال بعد می بینید که از وب سایتی ایمیل ارسال کرده و در این پایین می بینیم که تقریبا به صورت زیرکانه با وب سایت اصلی تفاوت دارد. یا در مورد بعدی می بینید که در قسمت پایین، یک تلفن از ایران گذاشته که مثلا بگوید من در کشور شما دفتر دارم اما در این قسمت گفته است که بر اساس سیاست های امنیتی شرکت ما، شما را در دیتابیس سایتمان گذاشته ایم و می توانید آن جا لاگین کنید و Orderهای خود را ببینید و یک Order هم داریم که می توانید با کلیک بر ر وی این لینک، آن ها را ببینید. تا به حال جایی دیده اید که کسی order خود را در لینک بگذارد؟ چه ایرادی داشت که order را خودش ارسال می کرد؟ زمانی می بینید که ایمیلی می آید، ارسال کننده اش درست است، متنش درست است، لینک عجیب و غریبی هم ندارد، وبسایتش هم معتبر است و تماس که می گیرد پاسخ می دهند اما از شما لیست قیمت می خواهند، شما هم لیست قیمت را برایش ارسال می کنید اما در انتها متوجه می شوید که از یک شرکت رقیب، اطلاعات شما را می گیرند تا بتواند با شما رقابت کند که همه اینها در بحث امنیت اطلاعات می گنجد.

لازم به ذکر است که همه مطالبی که در این قسمت بیان می شود، تجربی است و شاید علمی نباشد. به هیچ عنوان، ضمیمه ای جز JPG یا PDF را باز نکنید. هر فایل دیگری بود باز نکنید. فضای سفید در این ایمیل شاید به نظر برسد که چیزی نیست اما فقط کافی است که روی آن کلیک کنید. آیا اصلا شما منتظر دریافت پولی هستید که با دیدن TT Payment، یعنی زمانی که قرار است یک پیش پرداخت برای شما بیاید، به سراغ باز کردن ایمیل بروید؟ راحت ترین کار این است که این ایمیل ها را باز نکنید. هیچ کپی پرداختی به صورت Word ارسال نمی شود، یا JPG یا PDF است. اگر شک داشتید به همین مشتری ایمیل بزنید، ریپلای کنید و بگوید که JPG یا PDF آن را بفرست.

ایمیل هایی که بی ربط است، یعنی مستقیم برای شما ارسال می شود، برعکس آن چه که انتظار داریم. چون هکرهای حرفه ای، اول وب سایت شما را مطالعه می کنند و در نمایشگاه کارت شما را دریافت می کنند و بعد به آدرس ایمیل های Info ارسال می کنند. هکرهای حرفه ای با شما همزیستی می کنند. به هیچ عنوان هیچ ضمیمه ای را باز نکنید. اصلا ایمیل های بی ربط را باز نکنید و از همه بدتر، متأسفانه آن چه که رایج است ارسال صور قبیحه است یعنی از مطالبی استفاده می کنند که شاید برای کسی که می خواهد ایمیل را باز

کند جذابیتی داشته باشد. این ایمیل ها نشان می دهد که مستقیم به شرکت شما ایمیل می زنند و مطالب هم برای شما آشنا است که مثلا از طرف Purchase Officer، مسئول خرید ارسال می شود اما به این دلیل که مشخصات آن معلوم نیست باید برایمان مشکوک باشد. در این نمونه، آن چیزی که مشکل دارد وب سایت است، که آیا وارد این وب سایت بشویم یا نشویم و اگر شدیم چه لینک هایی روی آن موجود است. این ها را به عنوان نمونه نشان دادم که بگویم از این ایمیل ها زیاد است. پیشنهاد میدم یک کامپیوتر خودتان را بگذارید فقط برای جستجو در فضای اینترنت چراکه که به دنبال هر کلمه ای که بگردیم، ممکن است آن کلمه جذاب باشد و موتورهای جستجوگر بر آن تمرکز کنند و از طریق آن مورد حمله قرار گیرید.

در این خصوص، هکرها آخرین اتفاقی را که رقم می زنند، همزیستی است با Supplier. به عنوانم مثال، مشتری به عنوان واسطه، سفارشی را به شما می دهد و می گوید من با فلان خریدار ارتباط دارم و با ۲ درصد کمیسیون، این ارتباط را برقرار می کنم. وقتی من می گویم پسته دارم و علاقه من را به فروش می بیند می داند که باید از چه دروازه ای وارد سیستم من شود، معامله ای را منعقد می کند، با شما همزیستی می کند، محصول شما را به جایی می فروشد، شما کالایی را ارسال می کنید و اگر شانس بیاورید بار اول، ضربه خودش را می زند، شما کپی مدارک حمل را برای واسطه ارسال می کنید تا او آن مدارک را برای خریدار خارجی شما ارسال کند اما آدرس بانک را در زیر Proformaی شما عوض می کند در نتیجه شما این پول را از دست می دهید و ما قصد داریم این کار را تکرار نکنیم و حالا اگر هکر بدذاتی باشد، یک محموله، دو محموله و سه محموله به درستی با شما کار می کند و در نهایت Quantity و ارزش order را بزرگتر می کند و ضربه نهایی را در زمانی می زند که هست و نیست شما را ببرد. ما از این مدل ها باید بپرهیزیم، لذا تقاضا می کنیم دانش خودمان را، اطلاعات خودمان را، آن چه را می دانیم باهم به اشتراک بگذاریم. آن چه را که نمی دانیم یا سوال کنیم یا آن چه را که علم و تجربش را داریم به اطلاع دیگران برسانیم.

اما چطور می شود با هکری که همزیستی می کند مقابله کرد؟ رصد کردن آن ها بهترین روش است. یکی از بزرگترین مشکلاتی که ایجاد می شود این است که یک برند قوی یا یک شرکت مطرحی وجود دارد که واسطه است و ما هم دوست داریم با آن شرکت کار کنیم، هکر متوجه شده است که آن شرکت با ایران کار نمی کند، در نتیجه آدرس ایمیل هایی تعریف می کنند که آدرس ایمیل اصلی نیست به عنوان مثال آدرسی به عنوان info@cocacola.com می نویسد اما این ایمیل، اسمی است که برای آدرس خود تعریف کرده که این مسئله در Outlook این گونه است که یعنی اسم ارسال کننده ایمیل، این گونه است. پیشنهاد مشخص این است که شما باید با مشتری هدف خودتان، با حفظ احترام Broker، Trader و واسطه ها، یک سری مسائل را نهایی کنید که به عنوان مثال من به این واسطه احترام می گذارم اما آیا تو به عنوان خریدار اصلی، این واسطه را تأیید می کنی؟ یا از طریق مشتریان دیگر، او را رصد کنیم، قرار نیست به هر طریقی، جنسی را بفروشیم. ابزارهای ساده ای وجود دارد که بتوان یک مشتری را رصد کرد. اگر کسی قیمت محصولی را برای شرکت دیگری خواست، از خودش و از دیگران در مورد او سوال می کنم یعنی اعتبارسنجی می کنم که آیا می تواند منبعی برای تأیید خودش بدهد یا خیر.

در خصوص امنیت اطلاعات، A-۵، خط مشی های امنیت اطلاعات، به عنوان اولین بند، به دنبال ترغیب مدیر مجموعه در حرکت سازمان به سوی سیستم مدیریت امنیت اطلاعات است. جالب است که بدانید تمام کنترل های ایزو ۲۷۰۰۱ فقط توصیه می کند و ابدا الزامی را تحمیل نمی کند و شما می توانید قسمتی از موارد آن را اجرا کنید و قسمتی را حذف کنید اما به طور کلی می گوید مدیر مجموعه باید یک سری خط مشی هایی، Policy را برای مجموعه خود، توسعه دهد و بعد از تصویب آن، به تمام نیروها انتقال و آموزش دهد مانند کنترل دسترسی، طبقه بندی اطلاعات، میز پاک و صفحه نمایش پاک، پشتیبان گیری و امنیت ارتباطات.

به عنوان مثال، خط مشی گذرواژه با هدف انتخاب یک گذرواژه به منظور تضمین امنیت آن است بدین صورت که گذورواژه باید ده حرف داشته باشد و متشکل از حروف کوچک و بزرگ و کاراکترهای کنترلی باشد، اصطلاحات عامیانه و اطلاعات شخصی نباید به عنوان رمز انتخاب شود و یا می گوید که روش های متعددی را می توانید پیشنهاد دهید که چگونه گذرواژه خود را انتخاب کنند، به عنوان مثال یک جمله مرجع را در نظر بگیرید This May Be One Way To Remember! قسمت هایی که قرمز شده است را به عنوان گذرواژه انتخاب می کند و به رمزی می رسیم که شاید Complexity و سختی آن بالا باشد و قابل هک شدن نباشد. یا مثلا کلمه مرجع تابستان ۹۳$ را می توانید این گونه تایپ کنید که زبان کیبرد را انگلیسی کرده و فارسی تایپ کنید، این روش شاید مفید باشد اما هنگامی که مثلا با گوشی یا دستگاه دیگری می خواهید این رمز را تایپ کنید به مشکل بر می خورید و یا می توانید عبارتی را طراحی کنید که قسمت اول آن ترکیب اسم خودتان یا هر اسم دیگری باشد، قسمت دوم آن یک کارکتر کنترلی باشد، قسمت سوم عددی باشد که در ذهنتان به هر دلیلی باقی می ماند، قسمت چهارم یک کارکتر کنترلی دیگر، قسمت چهارم یک تاریخ مثلا یک سال مشخص، قسمت پنجم یک کارکتر کنترلی و بعد مخفف سایتی که قرار است برای آن رمزی بگذارید. مثلا GM برای Gmail یا YA برای Yahoo و یا به عنوان یک الزام می گوید برای سامانه های مختلف یک گذرواژه نگذارید که اگر یکی از آن ها هک شد، همه سامانه های شما از دسترس خارج نشود. یا بر اساس حساسیت شرکت شما، کارمندانتان را الزام کنید رمزهایشان را بین ۱۴ تا ۶۰ روز تغییر دهند. بعضی ها عادت دارند وقتی یک رمز را عوض می کنند، دوباره که قصد تعویض رمز را دارند، همان رمز قبلی را استفاده می کنند در صورتی که گفته می شود تا ۵ رمز قبلی را نباید تکرار کنید چراکه هکرها با استفاده از روش های امروزی ممکن است رمزهای قبلی شما را هم پیدا کنند. ثبت گذرواژه بر روی کاغذ یا به صورت الکترونیکی و بدون رمز انجام ندهید یا گذرواژه خود را با ایمیل و گفتگوی آنلاین به هم اعلام نکنید.

خط مشی میز پاک و صفحه نمایش پاک می گوید از دسترسی افراد غیرمجاز به اطلاعات موجود در مستندات روی میزها و اطلاعات قابل مشاهده از طریق صفحه نمایش جلوگیری کنید. این افراد نباید به برخی اطلاعات دسترسی داشته باشند اما از روی میزتان، کاغذها، پرونده ها یا حتی صفحه نمایشتان که باز است می توانند به اطلاعات زیادی برسند. در این حالت می توانید اطلاعاتتان را طبقه بندی کنید، اطلاعات محرمانه نباید هیچ وقت روی میزتان باشد یا هنگامی که به آن ها نیاز ندارید چرا باید در کنارتان روی میز باقی بماند؟ و باید آن ها را در کمد فلزی قفل دار بگذارید. یا مثلا صفحه نمایش نباید باز باشد که هر کسی داخل مجموعه شد از مشتریان و اطلاعات حساب شما مطلع شود. بر فرض هم که فراموش می کنید کامپیوتر خود را مدام lock کنید، آن را روی Auto lock بگذارید تا کسی نتواند به اطلاعات شما دسترسی پیدا کند.

یک سری عادت هایی وجود دارد که بسیار مخاطره آمیز است. به عنوان مثال عدم استفاده از آنتی ویروس های Original بسیار کار اشتباهی است و یک آنتی ویروس که به راحتی دانلود می شود حتی به روز هم که باشد به اندازه یک آنتی ویروس اصلی برای شما کارایی ندارد. به خاطر تحریم ها شاید نمی توانیم ویندوز اورجینال بخریم اما آنتی ویروس اورجینال وجود دارد و قیمت چندانی هم ندارد. از اطلاعات مهم تان حتما Back up بگیرید. اگر یک هکر وارد مجموعه شما شود و اطلاعات شما را به سرقت ببرد، باید فاتحه کسب و کارتان را بخوانید. علاوه بر این نرم افزارهای کرک شده که از هر جایی به دستتان می رسد را استفاده نکنید. یا از یک جای معتبر استفاده کنید یا ترجیحا از نرم افزاری استفاده کنید که برای ورود به آن نیاز به یک username & password باشد نه آن که فایل کرکی را در سیستم خود نصب کنید که در این صورت ممکن است آن فایل کرک، بلایی سر سیستم شما بیاورد. یا مثلا اتصال به شبکه های ناشناس و باز یا استفاده از یک فلش بدون استفاده از آنتی ویروس ممکن است سبب شود یک ویروس، worm یا تروجان وارد سیستم شما شود یا خیلی

مخفیانه، اطلاعات را از سیستم شما بردارند. یا برای کسانی که دورکاری می کنند و از راه دور برای شما کار می کنند، یک سری خط مشی برایشان تعریف کنید که به هر شبکه ای وصل نشود، هر ایمیلی نزد و ... این روزها خیلی فراگیر شده که اطلاعات را از طریق فضای مجازی به هر طریقی می فرستند اما باید بدانیم که این ها امنیت لازم را ندارند و ممکن است هک شود. یا استفاده از رمزهای دو مرحله ای، خیلی مرسوم نیست اما گوگل، لینکدین و یاهو رمزهای دو مرحله ای را ایجاد کرده اند به این صورت که هم یک password از شما می گیرند و هم یک پیام به گوشی شما ارسال می کنند. علاوه بر این اسناد مهم را بدون رمزنگاری برای هم ارسال نکنید و با Rar یا Veracrypt می توانید رمز بگذارید و یا یک آدرس ایمیل را به تمام سایت هایی که عضو هستید اعلام نکنید، Pop upهای مرورگرها را حتما block کنید چراکه از این طریق به راحتی می توانند فیشینگ کنند. به روزرسانی های خودکار ویندوز و آنتی ویروس را حتما به روز کنید، فکر نکنید اگر ویندوز به روز باشد مشقت زیادی برای شما ایجاد می کند، همچنین firewall ویندوز را به هیچ عنوان قطع نکنید، اولین جایی که از شما محافظت می کند، firewall ویندوز است که اگر خاموش باشد به راحتی به سیستم شما دسترسی پیدا می کنند و مهم تر از همه آن که گذرواژه هایتان را به کسی ندهید.

در این خصوص، مهندسی اجتماعی، یک تکنیک غیر فنی است که هکرهای امروزی و متخصصین مهندسی اجتماعی از یک راه غیرمعمول و ساده، در مجموعه شما رخنه می کنند و از طریق یک نفر، یک کارمند یا یک کاربر، ارتباطی می گیرند و به مجموعه شما مسلط می شوند اما شما متوجه نمی شوید. مثلا یک هکر از طریق یک تلفن یا اینترنت به سیستم شما دسترسی پیدا می کند و شما اصلا احتمال این مطلب را هم نمی دهید که از این طریق اطلاعات شما را به دست بیاورند. یا با استفاده از گرایشات طبیعی یک شخص مثلا علاقمندی به یک تیم مشترک و یا هر اشتراک دیگری می توانند با افراد، ارتباط برقرار کنند و به مجموعه شما ضربه بزنند. همگی موافقیم که کاربران، پیوند ضعیفی در امنیت هستند، اگر سیستم داشته باشید با یک آنتی ویروس می توانید جلوی آن را بگیرید اما در مورد نیروی انسانی به راحتی نمی توانید مقابله ای انجام دهید چراکه انسان احساسات دارد، عواطف دارد، با دیگران ارتباط دوستی دارد و ارتباط برقرار می کند و همین مسائل می شود محلی برای ضربه زدن.

هکرها با استفاده از افرادی که قاطی شدن و پدیدار شدن آن ها در مجموعه شان خیلی زیاد است به شما ضربه می زنند. مثلا نیروی حراست یا دربان شرکت که با همه ارتباط دوستی دارد، از همه خطرناک تر است، نه از این جهت که عمدی در ضربه زدن داشته باشد اما مهندس اجتماعی، از طریق او راحت تر می تواند کار خودش را پیش ببرد و به اطلاعات دسترسی پیدا کند. اما اگر می خواهید یک دفاع موفق داشته باشید باید یک خط مشی برای مجموعه خود تعریف کنید و یک سری رفتارها را حتما گوشزد کنید.

حملات مهندسی اجتماعی به طور کلی به دو طریق انجام می شود، یا متکی به انسان است یا متکی به کامپیوتر. در قسمت اول، با استفاده از تقلید صدای یک کاربر یا کارمند مورد تأیید و مهم که به آن Vishing – Voice Fishing می گویند بر اساس صحبت و Voice، به مجموعه شما وارد می شوند یا با استفاده از وانمود کردن به عنوان یک کاربر مهم وارد مجموعه می شوند که مثلا طرف خود را جای یکی از کارمندان معرفی می کند و از آن طریق وارد مجموعه می شود یا از تلفن و کامپیوترهای مجموعه استفاده می کند. یا با استفاده از تماس با پشتیبانی فنی مجموعه و تغییر شماره (Spoof) اینطور وانمود می کنند که یکی از اعضای مجموعه هستند و از آن طریق به شبکه نفوذ

می کنند. یا با مشاهده پسورد از روی دست شما یا استفاده از اطلاعات روی میز کار و زباله دان می توانند به اطلاعات زیادی دست پیدا کنند در نتیجه به نحوی اطلاعات را از بین ببرید که قابل دسترسی مجدد نباشد.

دسته دوم حملات از طریق اتکا به کامپیوتر صورت می گیرد مانند پیوست های ایمیل (Email attachment)، وبسایت های جعلی (Fake websites)، پنجره های پاپ آپ (Pop-up windows)، حمله از داخل و کارمندان خودی (Insider attack)، سرقت هویت (Identity theft)، حملات فیشینگ (Phishing attacks) و کلاهبرداری آنلاین (Online scams). گاهی اوقات با Replay بر روی یک ایمیل نامطمئن، کل سیستم در اختیار هکر قرار می گیرد یا با ظاهر شدن یک پاپ آپ در یک سایت، از شما می خواهند که وارد فیس بوک خود شوید یا مثلا از شما می خواهد flash player را به روز کنید یا هر روش دیگری که از طریق پاپ آپ صورت می گیرد که با کلیک بر روی آن ها، وارد سیستم شما می شوند.

یک نمونه از حملات فیشینگ به این صورت است که وقتی وارد یک هتل می شوید و از وای فای رایگان آن جا می خواهید استفاده کنید، آن وای فای می تواند محل ورود هکرها باشد بدین صورت که هکر، یک مودم در آن جا قرار می دهد و با ایجاد یک شبکه همانند شبکه هتل و استفاده شما از آن، اطلاعات شما را به سرقت ببرند در نتیجه به هر شبکه وای فایی متصل نشوید یا اگر متصل می شوید اطلاعات مهم مانند مشخصات کارت بانکی را در آن وارد نکنید یا فایل مهمی جابجا نکنید که همه این موارد، قابل هک شدن است.

به طور کلی امنیت اطلاعات تا آن جا مهم است که مارک زاکربرگ، مالک فیسبوک، خودش دوربین لپ تاپش را مسدود کرده چراکه خود آن ها نیز به هر شبکه ای اطمینان نمی کنند پس باید نکات زیادی را در این خصوص رعایت کنید به عنوان مثال با کامپیوتری که ایمیل ارسال می کنید، عملیات جستجو را انجام ندهید. بگذارید آن کامپیوترها فقط Outlookشان کار کند و برای جلوگیری از هک شدن ایمیل بهتر است در وبسایتتان یک شماره موبایلی را در نظر بگیرید که بتوانید به آن استناد کنید و زمانی که قرارداد را ارسال می کنید، با واتس آپ هم ارسال کنید و حتما یک بار شماره حساب بانکی را به صورت تلفنی با او چک کنید. حتی می توانید رمزهایی با مشتریان خود تعریف کنید تا شما را بشناسند و دیگران نتوانند خود را جای شما معرفی کنند.